UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/622,047	08/23/2000	Alexandr Andreevich Moldovyan	P65855US0	4150

136 7590 09/30/2008

JACOBSON HOLMAN PLLC
400 SEVENTH STREET N.W.
SUITE 600
WASHINGTON, DC 20004

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2132	
MAIL DATE	DELIVERY MODE
09/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ALEXANDR ANDREEVICH MOLDOVYAN,
NIKOLAY ANDREEVICH MOLDOVYAN, and
NIKOLAY VIKTOROVICH SAVLUKOV

Appeal 2008-1929
Application 09/622,047
Technology Center 2100

Decided: September 29, 2008

Before JAMES D. THOMAS, JEAN R. HOMERE, and THU A. DANG, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF CASE

Appellants appeal the Examiner's final rejection of claims 1, 3, and 5 under 35 U.S.C. § 134. We have jurisdiction under 35 U.S.C. § 6(b).

A. INVENTION

According to Appellants, the invention pertains to the field of electrical communication and computer technology. More precisely, it relates to cryptographic methods for encrypting messages (information). (Spec. 1, ll. 2-4).

B. ILLUSTRATIVE CLAIM

Claim 1 is exemplary and is reproduced below:

1. A method for block encryption of discrete data, comprising the steps of: generating an encryption key in the form of a set of subkeys, breaking down a data block into $N \geq 2$ data subblocks and alternately converting said data subblocks by performing a two-place operation on the data subblock and the subkey, wherein, prior to carrying out said two-place operation on an i-th data subblock and a subkey, an operation of permuting subkey bits is performed on the subkey depending on the value of a j-th data subblock, where $i \neq j$.

C. REJECTIONS

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Schneier, Bruce, *Data Encryption Standards (DES)*, Applied Cryptography, Second Edition, John Wiley & Sons, 270-275 (1996).

Claims 1, 3, and 5 stand rejected under 35 U.S.C. § 102(b) over the teachings of Schneier.

We affirm.

II. ISSUES

The issues are whether Appellants have shown that the Examiner erred in finding that claims 1, 3, and 5 are anticipated under 35 U.S.C. § 102(b) by the teachings of Schneier, and in particular, that Schneier discloses the claimed limitation of, prior to carrying out said two-place operation on an i-th data subblock and a subkey, an operation of permuting subkey bits is performed on the subkey depending on the value of a j-th data subblock (Claim 1).

III. FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

Schneier

1. Schneier discloses DES (US Data Encryption Standard) which operates on a 64-bit block of plaintext. After an initial permutation, the block is broken into a right half and a left half. There are 16 rounds of identical operations, called Function f, in which the data are combined with a key. After the sixteenth round, the right and left halves are joined, and a final permutation finishes off the algorithm (pg. 270, Sect. 12.2).
2. In each round of permutation in Schneier, the key bits are shifted, and then 48 bits are selected from the 56 bits of the key. The right half of the data is expanded to 48 bits via an expansion permutation,

combined with 48 bits of a shifted and permutted key via an XOR, sent through 8 S-boxes producing 32 new bits, and permutted again. These four operations make up Function f (pg. 270, Sect. 12.2; Fig. 12.2).

PRINCIPLES OF LAW

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros., Inc. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987).

The *claims* measure the invention. *See SRI Int'l v. Matsushita Elec. Corp., of America*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). "[T]he PTO gives claims their 'broadest reasonable interpretation.'" *In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000)). "Moreover, limitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) (citing *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989)).

V. ANALYSIS

Appellants do not provide separate arguments with respect to the rejection of claims 1, 3, and 5. Therefore, we select independent claim 1 as being representative of the cited claims. 37 C.F.R. § 41.37(c)(1)(vii).

Appellants argue that "Schneier, when describing algorithm DES (US Data Encryption Standard), does not disclose any feature of converting a subkey depending on data being converted" (App. Br. 4) but instead "round keys K_1, K_2, …, K_{16} are generated by means of converting a secret key, on which an operation of fixed transmuting key bits is performed, which depends on the round number but **does not depend on data subblock being converted**" (App. Br. 5). Appellants argue that "the conversion operation *f* is not an operation of permutation" (App. Br. 6), and that "in algorithm DES, the **bit permutation operation** is performed on the key by **depending on the number of the round, but not on the data subblock**" (App. Br. 7).

We begin our analysis by giving the claims their broadest reasonable interpretation. *See In re Bigio* at 1324. Furthermore, our analysis will not read limitations into the claims from the specification. *See In re Van Geuns* at 1184.

Appellants' argument that Schneier does not disclose "converting a subkey depending on data being converted" because Schneier discloses "converting a secret key, on which an operation of fixed transmuting key bits is performed, which depends on the round number" is not commensurate with the invention that is claimed. That is, such "converting" step is not recited in the claimed invention, and thus, cannot be read into the claims as the Appellants argued. Further, Appellants appear to be arguing that because Schneier discloses converting a secret key by depending on the round number, Schneier does not disclose converting a subkey *only*

depending on data being converted. Such *converting only* depending on data being converted limitation cannot be read into the claims and such argument is not commensurate with the claimed invention. Accordingly, the issue is whether Schneier discloses the claimed limitation of, prior to carrying out a two-place operation on a data subblock and a subkey, permuting subkey bits depending on the value of a data subblock (Claim 1).

The Examiner finds that Schneier discloses the claimed elements on appeal as set forth beginning at page 2 of the Answer, and provides responsive arguments beginning at page 4 of the Answer. We agree.

Schneier discloses a DES algorithm which operates on a 64-bit block broken into a right half and a left half, the algorithm comprising 16 rounds of identical operations, Function f, combining data with a key, wherein, after the sixteenth round, the right and left halves are joined, and a final permutation finishes off the algorithm (FF 1). Further, making up Function f in each round, the right half of the data is expanded to 48 bits via an expansion permutation, combined with 48 bits of a shifted and permutted key via an XOR, sent through 8 S-boxes producing 32 new bits, and permutted again (FF 2). In the Examiner's Answer, the Examiner references Fig. 12.1 of Schneier and finds that, in each round of the DES of Schneier, "the data subblock Lo is exclusive or'd with the result of the permutation function on subkey Ki that depends on data subblock Ro" where "Lo would meet the limitation of the i-th data subblock, Ro would meet the limitation of the j-th data subblock, K1 would meet the limitation of the subkey being

permutted, and function f would meet the limitation of the permutation function" (Ans. 3).

We find the various permutations of the right and left halves including the data subblocks and subkeys during each of the sixteen rounds to be carrying out a two-place operation on a data subblock and a subkey. We agree with the Examiner's finding that, contrary to the Appellants' assertion, the Function f of a current data subblock is a permutation function performed prior to carrying out a two-place operation of a subsequent data subblock, wherein a subkey is permutted depending on the current data subblock. That is, as set forth in Schneier, Function f consists of four operations which *includes* permutation of the data subblock and key (FF 2), wherein Function f depends on a data subblock for its performance.

Though Appellants argue that Schneier discloses "converting a secret key, on which an operation of fixed transmuting key bits is performed, which depends on the round number," we agree with the Examiner that the operation of Function f on the data subblock and subkey, as taught by Schneier, is *also* permuting subkey bits depending on the value of a data subblock, as recited in claim 1. That is, Function f, which includes permuting subkey bits, depends on the data subblock and subkey since it is performed on both the data subblock and subkey, and thus, the permutation of the subkey bits *depends* on the value of the data sublock.

In the Reply Brief, Appellants add the argument that the operation in Schneier "is a fixed permutation operation which is not a permutation

operation that depends on data being converted" (Reply Br. 6). However, such argument is not commensurate with the invention that is claimed. That is, Appellants appear to be arguing because Schneier discloses a fixed permutation, Schneier does not disclose permuting *only* depending on data being converted. As discussed above, such *only* limitation cannot be read into the claims and such argument is not commensurate with the claimed invention.

Contrary to the Appellants' assertion, even if Schneier also discloses "a fixed permutation," as Appellants argue, we agree with the Examiner that the operation of Function f on the data subblock and subkey, as taught by Schneier, is *also* permuting subkey bits depending on the value of a data subblock as recited in claim 1. As discussed above, Function f, which includes permuting subkey bits, is performed on both the data subblock and subkey, and thus, the permutation of the subkey *depends* on the value of the data sublock.

Accordingly, we conclude that Schneier discloses the claimed limitation of, prior to carrying out said two-place operation on an i-th data subblock and a subkey, an operation of permuting subkey bits is performed on the subkey depending on the value of a j-th data subblock (Claim 1), and that Appellants have not shown that the Examiner erred in rejecting claim 1 and claims 3 and 5 falling with claim 1 under 35 U.S.C. § 102(b).

CONCLUSIONS OF LAW

(1) Appellants have not shown that the Examiner erred in finding that claims 1, 3, and 5 are anticipated by the teachings of Schneier.

(2) Claims 1, 3, and 5 are not patentable.

DECISION

We affirm the Examiner's rejection of claims 1, 3, and 5 under 35 U.S.C. § 102(b).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

rwk

JACOBSON HOLMAN PLLC
400 SEVENTH STREET N.W.
SUITE 600
WASHINGTON DC 20004